5.4.X InBandDigits Message

The InBandDigits message shall report intercept subject inputs detected by the accessing switch that has partially or fully cut-through a call content path from the subject toward an associate. The inputs reported include any DTMF tones detected. Inputs may be accumulated and sent when there is a significant pause between inputs or when an event precludes acting upon the input, such as call abandonment. A Delivery Function separate from the Access Function may perform extraction of digits from a CCC and insertion of digits into an InBandDigits message on the CDC.

The InBandDigits message shall be triggered when a string of DTMF digits is detected following cut-through.

The InBandDigits message includes the following parameters:

Table X: InBandDigits Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
UserInput	M	Identifies specific user input when it is detected.

c. **Section 6.3 CDC Message Definitions:** Add the following message definition:

6.3.X InBandDigits

The InBandDigits message reports in-band user input following cut-through of the subject's talk path.

```
InBandDigits :: = SEQUENCE {
                        [0]     CaseIdentity,
                        [1]     IAPSystemIdentity           OPTIONAL,
                        -- Include to identify the system containing the IAP  when the
                        -- underlying data carriage does not imply that system.
                        [2]     TimeStamp,
                        [3]     CallIdentity,
        userInput       [4]     VisibleString (SIZE (1..32) )
                        -- e.g., "12345" or "*123" or "#345" or "KEY1"
}
```

16. Problem: Law enforcement is not provided all call-identifying information for a call.

Recommendations:

a. **Section 4.4 Call Associated Information Surveillance Service Description—Call Identifying Information IAP:** Add the following to the existing list of call events:

Notification

The subject or an associate is signaled by the subject's service.

b. **Section 5.4:** Add the following message:

5.4.X Notification Message

The Notification message shall report out-of-band signaling delivered through a subject's service that can be sensed by the intercept subject or an associate communicating with the subject's service. The Notification message is also used to report in-band signaling applied by the accessing system.

The Notification message shall be triggered when:

- The accessing system applies an in-band audible indication to the *intercept subject's* receive content channel or sends or passes a command to the *intercept subject's* terminal to activate, deactivate, or control generation of the following:
  - Any alerting of incoming calls or messages
  - Audible indications (e.g., call waiting tone, message waiting tone, power alert/ringing, distinctive alert/ringing, recall alert/dial tone, or call forwarding reminder alert/ring, busy tone, or reorder tone)
  - Visual indications (e.g., lights to indicate call waiting)
  - Alphanumeric display information (e.g., messages sent by the switch or permanently stored in the terminal, calling number identification, or calling name identification).
- The accessing system, for incoming call attempts to a subject, in support of communications with the intercept subject, applies an in-band audible indication to the *associate's* receive channel, or sends or passes a command to the *associate's* terminal to activate, deactivate, or control generation of call progress tones (e.g., ring-back or busy tones).

The Notification message includes the following parameters:

Table X: Notification Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
Signaled Party	M	Identifies the signaled party.
Audible Visual or Displayed Signal	M	Identifies the audio signal, visual signal, or displayed text.

c. **Section 6.3 CDC Message Definitions:** Add the following message definition:

6.3.X Notification

The Notification message reports out-of-band and in-band signals related to the subject's service that are generated or delivered by the accessing system toward a subject or an associate. This includes commands to control alerting, tone generation, and alphanumeric displays.

```
Notification :: = SEQUENCE {
                        [0]     CaseIdentity,
                        [1]     IAPSystemIdentity           OPTIONAL,
                        -- Include to identify the system containing the IAP  when the
                        -- underlying data carriage does not imply that system.
                        [2]     TimeStamp,
                        [3]     CallIdentity,
        signaledParty   [4]     PartyIdentity,
audioVisualDisplay      [5]     VisibleString (SIZE (1..128) )
}
```

17. Problem: No mechanism exists to provide law enforcement timely notification when an intercept subject is assigned or activates new features in the network. Absent such a mechanism, it is possible that law enforcement may not have established sufficient delivery capabilities to receive all the intercepted communications or call-identifying information. The following is one way to address the problem.

Recommendations:

a. Add new **Section 4.3.2: Feature Status IAP:**

The Feature Status IAP reports with a Feature Status message when an intercept subject first gains the ability to invoke network-provided features that would affect the delivery to law enforcement of call content or call-identifying information related to that subject. Those features are described in more detail in Stage 2.

The Feature Status message is required to report features affecting lawfully authorized surveillance that are assigned or removed as a result of service provider actions or that are activated or deactivated remotely, using another subscriber's equipment, facilities, or services.

The Feature Status message does not need to be reported when new features affecting lawfully authorized surveillances are assigned, activated, deactivated, or removed through the use of the subject's equipment, facilities, or services. In these situations, changes are detectable through other messages described in this standard.

b. **Section 5.4:** Add the following message:

5.4.X FeatureStatus Message

The FeatureStatus message shall report when an intercept subject first gains or loses the ability to invoke, without delay, network-provided features that would affect the delivery to law enforcement of call content or call-identifying information related to that subject. The FeatureStatus message is not required when a new capability is gained through the subject's terminal and is reported by other LAES messages.

The FeatureStatus message shall be triggered when the service provider assigns or removes and when the subject activates or deactivates the following features:

- Call redirection features that affect the routing of calls, including all variations of call forwarding features (e.g., call forwarding busy and call forwarding unconditional)
- Multiple circuit features that affect the number of CCCs required to include all variations of multiparty features (e.g., call waiting, call hold, three-way calling, conference calling)
- Features that affect surveillance trigger identities (e.g., number change feature)
- Service suspend and service disconnect features.

The FeatureStatus message includes the following parameters:

Table X: FeatureStatus Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
FeatureName	M	Identifies the feature or service.
FeatureModification	M	Identifies the type of successful feature change.
FeatureParties	C	Included when the feature involves association of parties to the feature.

c. **Section 6.3 CDC Message Definitions:** Add the following message definition:

6.3.X FeatureStatus

The FeatureStatus message reports a remote request by an intercept subject or the service provider, for assignment, removal, activation, or deactivation of network-provided features identified in Stage 2 that would adversely affect the delivery to law enforcement of call content or call-identifying information related to the subject.

```
FeatureStatus :: = SEQUENCE {
                    [0]   CaseIdentity,
                    [1]   IAPSystemIdentity                OPTIONAL,
                    -- Include to identify the system containing the IAP  when the
                    -- underlying data carriage does not imply that system.
                    [2]   TimeStamp,
    featureName     [3]   VisibleString (SIZE (1..64) ),
                    [4]   FeatureModification,
    featureParties  [5]   SEQUENCE OF PartyIdentity        OPTIONAL
                    -- included when feature usage records other party identities
}
```

d. **Section 6.4 CDC Parameter Definitions:** Add the following parameter definition:

6.4.X FeatureModification

The FeatureModification parameter indicates only successful modifications to an intercept subject's capabilities.

```
FeatureModification ::= ENUMERATED {
                        assignment                      (0),
                        unassignment                    (1),
                        activation                      (2),
                        deactivation                    (3),
                        changeOfAssocitatedPartyIdList  (4)
}
```

18. Problem: No mechanism is specified to ensure surveillance integrity. No mechanism exists to notify law enforcement when an interception is activated, deactivated, or fails. Such a mechanism is imperative because the carrier will be performing the access and delivery. The failure to provide law enforcement with a timely mechanism to indicate that a carrier's network-based (e.g., switch-based) interception of a surveillance subject has been activated or deactivated removes the most elementary evidentiary aspect of conducting electronic surveillance: Is the interception working ("live" or "active") or not, and when was it working?

Recommendations:

a. Add **new Section 4.3.3: Surveillance Status IAP:**

> The Surveillance Status IAP shall report with a SurveillanceStatus message the status of a surveillance for a particular subject whenever a surveillance is activated, updated, or deactivated. The SurveillanceStatus message shall also be sent periodically from once every hour to once every 24 hours for the duration of a surveillance. The Surveillance Status IAP and message confirm the integrity of the lawfully authorized surveillance, including indications when a subject's service has been terminated (disrupted) or that the interception, as effected by the carrier, has been terminated (disrupted) intentionally or inadvertently.

b. **Section 5.4:** Add the following message:

5.4.X SurveillanceStatus Message

The SurveillanceStatus message reports when a surveillance for a subject is activated, updated, or deactivated. The SurveillanceStatus message is also sent periodically from once every hour to once every 24 hours during a surveillance. The activate and update status messages shall report any call content channels assigned to the surveillance.

The SurveillanceStatus message shall be triggered when:

- The surveillance is activated, updated, or deactivated
- Periodically for the duration of the surveillance.

The SurveillanceStatus message includes the following parameters:

Table X: SurveillanceStatus Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
SurveillanceStatusType	M	Identifies the type of SurveillanceStatus report.
Provisioned CCCs	C	Included when call content channels are provisioned.

c. **Section 6.3 CDC Message Definitions:** Add the following message definition:

6.3.X SurveillanceStatus

The SurveillanceStatus message reports when a surveillance for a subject is activated, updated, deactivated, and periodically during the surveillance. The period shall be provisioned to be from once every hour to once every 24 hours. Updates concern changes to the number and identity of CCCs provisioned for the particular CaseIdentity.

```
SurveillanceStatus :: = SEQUENCE {
                        [0]    CaseIdentity,
                        [1]    IAPSystemIdentity                    OPTIONAL,
                        -- Include to identify the system containing the IAP when the
                        -- underlying data carriage does not imply that system.
                        [2]    TimeStamp,
                        [3]    SurveillanceStatusType,
   provisionedCCCs      [4]    SEQUENCE OF EXPLICIT CCCIdentity     OPTIONAL
}
```

d. **Section 6.4 CDC Parameter Definitions:** Add the following parameter definition:

6.4.X SurveillanceStatusType

The SurveillanceStatusType parameter indicates the type of status reported.

```
SurveillanceStatusType ::= ENUMERATED {
                                activated     (0),
                                updated       (1),
                                inProgress    (2),
                                deactivated   (3)
}
```

19. Problem: No mechanisms are defined to ensure CCC integrity. It is possible that CCC circuit failures could be undetectable by law enforcement for a period of time. An in-band tone, such as DTMF C-tone, is required for continuity assurance.

Recommendations:

a. **Section 6.5 CCC Protocols:** Add the following CCC requirements:

> When dedicated circuits are used to support CCCs ("nailed-up" CCCs), a continuous signal or tone (such as DTMF C-tone) shall be applied to idle CCCs to verify continuity.

b. **Section B.3.4 CCC Continuity Verification:** Page 74, lines 19-22: Add the following text:

> When the CIAP detects that an intercept subject is requesting service (i.e., going off-hook), the continuous signal or tone (such as DTMF C-tone) should be dropped to allow call content to be delivered.

c. **Section B.4.4 CCC Continuity Verification:** Page 89, line 9: Add the following text:

> Law enforcement recommends using continuous DTMF C-tone as the test signal. DTMF C-tone should be applied when the trunk is idle and removed when call content is delivered.

20. Problem: SP-3580A does not specify standards for supporting protocols for the CDC physical interface for the delivery of call-identifying information to law enforcement.

Recommendations:

a. **Section 6.2.1 CDC Underlying Data Transmission:** Law enforcement recommends that X.25 or one suitable alternative standard be specified. Add the following text to address data transfer service for the CDC:

> This standard does not specify underlying data communications protocols to support CDC message transmission within a service provider's network.
>
> CALEA, section 103(a)(3) requires delivery of call-identifying information to the government "in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier."
>
> CDC messages shall be delivered within X.25 data packets across the demarcation point between a service provider network and government-procured facilities. The X.25 protocol was selected because it is a standard, widely deployed, and mature network access protocol. X.25 and supporting protocols shall be used over both analog and digital DS1 wireline interfaces to law enforcement.
>
> The TSP shall support the CDC using an X.25 interface that conforms to ITU-T Recommendation X.25.
>
> CDC messages shall be encapsulated in the user data field of X.25 data packets, as defined in ITU-T Recommendation X.25.
>
> The X.25 packet layer shall support logical channel assignments, consistent with Section 3.1 of ITU-T Recommendation X.25.
>
> The X.25 interface shall support the modulo-8 data packet sequence numbering, as described in Section 4.4.1.1 of ITU-T Recommendation X.25.
>
> The following default X.25 packet layer parameters shall be supported:
>
> | | |
> |---|---|
> | Connection: | Switched or Permanent Virtual Circuit |
> | Packet Sequencing: | Modulo 8 (Modulo-127 Optional) |
> | Logical Channels: | 1 per surveillance |
> | Minimum Packet Size: | 128 octets |
> | Window Size: | 2 (extensible to modulo-N minus 1) |
> | User Data Alignment: | Octet aligned. |
>
> The X.25 interface shall support a data packet size of at least 256 octets.

The X.25 interface shall support the procedures associated with the use of the Delivery Confirmation Bit (D bit) for end-to-end acknowledgment of packet delivery as described in Section 4.3.3 of ITU-T Recommendation X.25. The D bit shall be set to 1 in packets containing CDC messages.

The X.25 interface shall support the procedures associated with the complete packet sequence mechanism, as described in Section 4.3.5 of ITU-T Recommendation X.25.

The X.25 interface shall support the procedures associated with the use of the Qualifier bit (Q bit), as described in Section 4.3.6 of ITU-T Recommendation X.25. The Q bit shall be set to 0 in packets containing CDC messages.

The X.25 interface shall support the Link Access Protocol-B (LAPB) procedures, as defined in Section 2 of ITU-T Recommendation X.25 for the data link layer control. The default values shall be supported for the LAPB system parameters, as defined in Section 2.4.8; and in particular, the Single Link Procedure (SLP) shall be supported.

b. **Section A.4 Implementation of the e-interface:** Several different protocols could be supported over the e-interface; however, failure to mandate a limited number of protocols for the e_4-interface and to define explicit standard protocol requirements would have managerial and cost implications for the Collection Function. **Section A.5 Possible CDC Protocol Stacks:** Page 66, line 5: Add the following text:

The protocols for the e_4-interface shall be limited to X.25 with supporting LAPB link layer and DS1 physical layer (or V.32 over an analog facility). The virtual connection method used for the X.25 interface should be either a Permanent Virtual Circuit (PVC) or a Switched Virtual Call service (SVC). PVC allows a virtual connection to remain active for the duration of the surveillance. An SVC allows a virtual connection to be created when call-identifying information is available for delivery. The X.25 data link layer should support Link Access Procedures for B channel interfaces (LAPB) and for D channel interfaces (LAPD). The X.25 physical layer should support X.21, X.21 bis and V-Series interfaces.

21. Problem: Several different protocols could be supported over the e-interface; however, failure to mandate a limited number of protocols and to define explicit standard protocol requirements would have managerial and cost implications for the Collection Function. There are no specifications regarding the format of delivery of call content to law enforcement. SP-3580A does not specify standards for supporting protocols for the CCC physical interface.

Recommendations:

a. **Section 6.5 CCC Protocols:** Add the following CCC requirements:

> For both circuit-mode and packet-mode services, the CCC shall support interconnection to and transmission over an analog wireline circuit or digital DS1 wireline circuit at the demarcation point.
>
> On an analog wireline e-interface, CCCs shall be as specified in widely used standards or technical requirements.
>
> On a DS1 physical e-interface, CCCs shall use time-multiplexed signals as specified in ANSI T1.107-1995 and shall support electrical interfaces for the CCCs as specified in ANSI T1.102-1993.

b. **Section A.6 Possible CCC Protocol Stacks:** Section A.6, Page 68, line 46: Add the following text:

> CCCs are exported from the accessing network over dedicated trunk facilities or demand access facilities. On digital IAP switches, these facilities shall be digital, multiplexed interfaces such as the metallic DS1 interface. On analog IAP switches, these facilities shall be analog trunk interfaces.

Annex D Information Access Scenarios:

22. Problem: **Section D.7.3** and **Section D.10.3** illustrate call content on a CCC being temporarily withheld when an associate is alone on hold (Steps 5 through 7); however, there is no requirement in the normative part of the standard for that capability.

    Recommendation: Add to **Section 4.5.1:** "If separate call identities and CCCs are maintained for individual call legs (i.e., parties) of a subject-initiated multiparty call, the party's call content shall be delivered over the CCC only when the intercept subject or another party of the multiparty call is capable of receiving such call content."

23. Problem: Maintain consistency with decisions on messages in the body of SP-3580A.

    Recommendations:

    a. **Section D.3 Pre-Answer Abandon:** Add Notification messages for network signals applied toward the intercept subject and Party A.

    b. **Section D.4 Simple Outgoing Call:** Add Notification messages for network signals applied toward the intercept subject and Party A and add the InBandDigits message including the subject's input.

    c. **Section D.5 Re-Origination:** Add Notification messages for network signals applied toward the intercept subject and Parties A and B.

    d. **Section D.6 Simple Incoming Call:** Add Notification messages for network signals applied toward the intercept subject and Party A.

    e. **Section D.7.1 Call Waiting and Recall with a Single Call Identity:** Add Notification messages for network signals applied toward the intercept subject and Parties A and B. Add the Origination message including subject's "flash" signal and add PartyHold, PartyJoin, PartyDrop, or Change messages to indicate CCC identity changes or party identity changes with respect to call identity.

    f. **Section D.7.2 Call Waiting and Recall with Separate Leg Identities:** Add Notification messages for network signals applied toward the intercept subject and Parties A and B. Add the Origination message including subject's "flash" signal and add PartyHold, PartyJoin, PartyDrop, or Change messages to indicate CCC identity changes or party identity changes with respect to call identity.

    g. **Section D.7.3 Call Waiting and Recall with Separate Calls:** Add Notification messages for network signals applied toward the intercept subject and Parties A and B. Add the Origination message including subject's "flash" signal and add PartyHold, PartyJoin, PartyDrop, or Change messages to indicate CCC identity changes or party identity changes with respect to call identity.

h. **Section D.8.1 Call Waiting with Talking Party Disconnect and a Single Call Identity:** Add Notification messages for network signals applied toward the intercept subject and Parties A and B. Add the Origination message including subject's "flash" signal and add PartyHold, PartyJoin, PartyDrop, or Change messages to indicate CCC identity changes or party identity changes with respect to call identity.

i. **Section D.8.2 Call Waiting with Talking Party Disconnect and Separate Leg Identities:** Add Notification messages for network signals applied toward the intercept subject and Parties A and B. Add the Origination message including subject's "flash" signal and add PartyHold, PartyJoin, PartyDrop, or Change messages to indicate CCC identity changes or party identity changes with respect to call identity.

j. **Section D.8.3 Call Waiting with Talking Party Disconnect and Separate Calls:** Add Notification messages for network signals applied toward the intercept subject and Parties A and B. Add the Origination message including subject's "flash" signal and add PartyHold, PartyJoin, PartyDrop, or Change messages to indicate CCC identity changes or party identity changes with respect to call identity.

k. **Section D.9 Call Held and Retrieved:** Add Notification messages for network signals applied toward the intercept subject and Parties A and B. Add the Origination message including subject's "hold" signal and add PartyHold, PartyJoin, PartyDrop, or Change messages to indicate CCC identity changes or party identity changes with respect to call identity.

l. **Section D.10.1 Three-Way Calling, Plus Call Turned Away with a Single Call Identity:** Add Notification messages for network signals applied toward the intercept subject and Parties A, B, and C. Add the Origination message including subject's "flash" signal and add PartyHold, PartyJoin, PartyDrop, or Change messages to indicate CCC identity changes or party identity changes with respect to call identity.

m. **Section D.10.2 Three-Way Calling, Plus Call Turned Away with Separate Leg Identities:** Add Notification messages for network signals applied toward the intercept subject and Parties A, B, and C. Add the Origination message including subject's "flash" signal and add PartyHold, PartyJoin, PartyDrop, or Change messages to indicate CCC identity changes or party identity changes with respect to call identity.

n. **Section D.10.3 Three-Way Calling, Plus Call Turned Away with Separate Calls:** Add Notification messages for network signals applied toward the intercept subject and Parties A, B, and C. Add the Origination message including subject's "flash" signal and add PartyHold, PartyJoin, PartyDrop, or Change messages to indicate CCC identity changes or party identity changes with respect to call identity.

o. **Section D.11 Call Forwarding—No Answer on a Single System:** Add Notification messages for network signals applied toward the intercept subject and Party A.

p. **Section D.12 Call Forwarding—No Answer on a Different System:** Add Notification messages for network signals sent to the intercept subject and Party A.

q. **Section D.13 Two Bearer Channels, Plus Call Transfer:** Add Notification messages for network signals applied toward the intercept subject and Parties A, B, and C. Add the Origination message including subject's "transfer" signal and add PartyDrop, or Change messages to indicate CCC identity changes or party identity changes with respect to call identity.

r. **Section D.14 Speed Calling:** Add Notification messages for network signals applied toward the intercept subject and Party A.

s. **Section D.15 Multiple Translations on Single System:** Add Notification messages for network signals applied toward the intercept subject and Party A.

t. **Section D.16 Multiple Call Scenario:** Add Notification messages for network signals applied toward the intercept subject and Parties A, B, and C.

u. **Section D.17 Simple Call Delivery to a Mobile Station:** Add Notification messages for network signals applied toward the intercept subject and Party A and add the ServingSystem message indicating the subject's registration.

v. **Section D.18 Password Call Acceptance and Flexible Alerting:** Add Notification messages for network signals applied toward the intercept subject and Parties A and B.

w. **Section D.19 Password Call Acceptance and Call Forwarding:** Add Notification messages for network signals applied toward the intercept subject and Parties A and B.

x. **Section D.20 Completed Call to Busy Subscriber:** Add Notification messages for network signals applied toward the intercept subject and Party A.

y. **Section D.22, Call Release to Pivot:** Add Notification messages for network signals applied toward the intercept subject and Party A.

INTERIM STANDARD
(TRIAL USE STANDARD)

J-STD-025

Lawfully Authorized Electronic Surveillance

J-STD-025

DECEMBER 1997

Jointly Developed by:

TELECOMMUNICATIONS TIA INDUSTRY ASSOCIATION

In Association with the

Sponsored by the

Alliance for Telecommunications

INTERIM STANDARDS

Interim Standards (Trial Use Standards) contain information deemed to be of technical value to the industry, and are published at the request of the originating Committee without necessarily following the rigorous public review and resolution of comments which is a procedural part of the development of a American National Standard.

Under TIA Engineering Manual, Interim Standards should be reviewed on an annual basis by the formulating Committee and a decision made on whether to proceed to develop a American National Standard on this subject. Interim Standards must be cancelled by the Committee and removed from the Standards Catalog before the end of their third year of existence.

Publication of this Interim Standard for trial use and comment has been approved by the Telecommunications Industry Association. Distribution of this Interim Standard for comment shall not continue beyond 36 months from the date of publication. It is expected that following this 36-month period, this Interim Standard, revised as necessary, will be submitted to the American National Standards Institute for approval as an American National Standard. Suggestions for revision should be directed to: Standards Secretariat, Standards & Technology Department, Telecommunications Industry Association, 2500 Wilson Boulevard, Arlington, VA 22201.

Standards and Publications are adopted in accordance with the American National Standards Institute (ANSI) patent policy. By such action, TIA or ATIS does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard or Publication.

(From Project No. 4116, formulated under the cognizance of the TIA TR-45.2 and Committee T1.)

Published by

©TELECOMMUNICATIONS INDUSTRY ASSOCIATION 1997
Standards & Technology Department
2500 Wilson Boulevard, Suite 300
Arlington, VA 22201
or
©Alliance for Telecommunications Industry Solutions
1200 G Street, NW
Suite 500
Washington, DC 20005
(202) 628-6380

Contents

List of Tables

List of Figures